Applicant: David Grawrock et al.
Serial No.: 09/934,926, filed 08/21/01
Atty Docket No.: SYMA-01045US0MCF/GGG

Fig. 1A

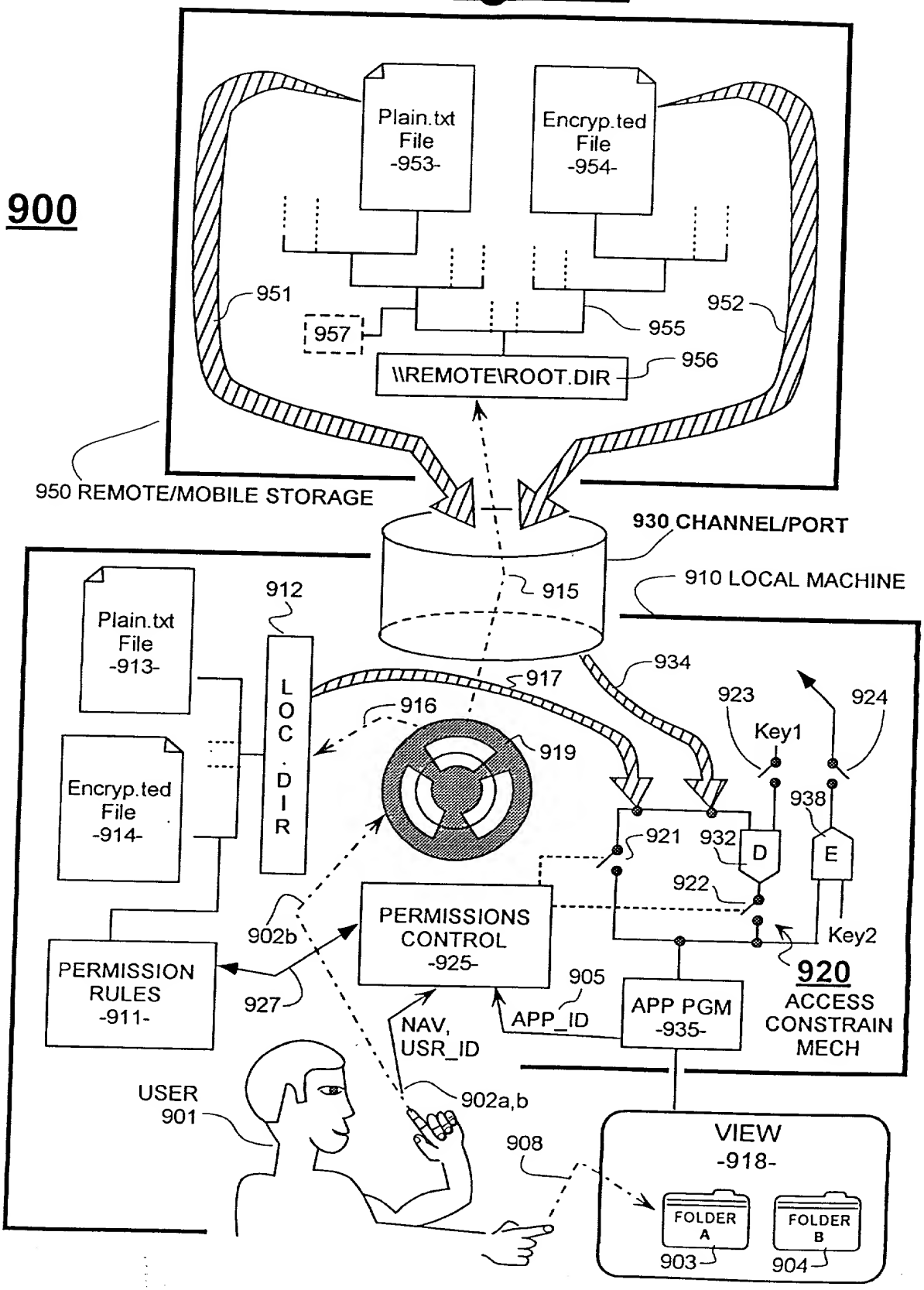


Fig. 1B

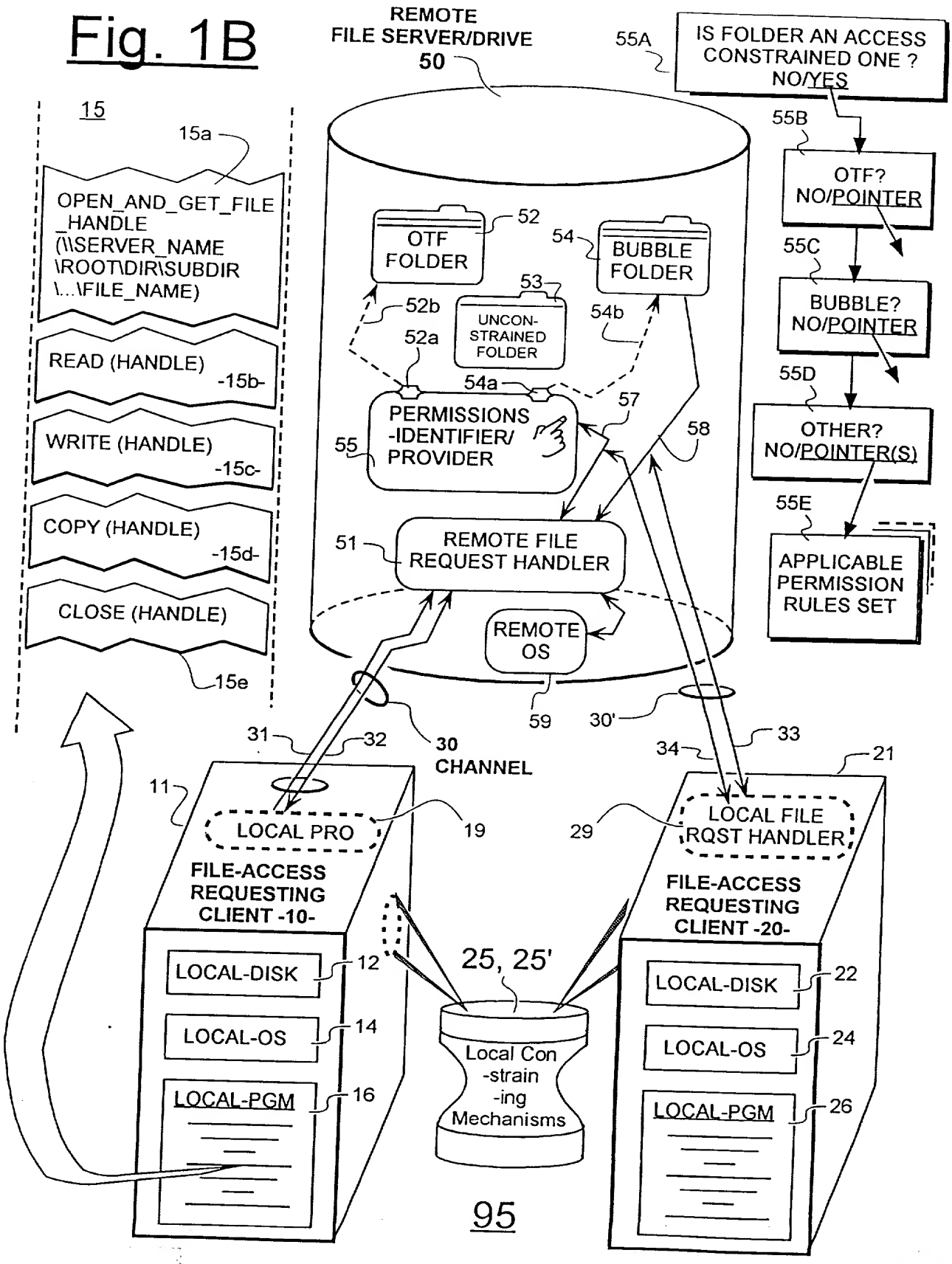

REMOTE
FILE SERVER/DRIVE
50
55A
IS FOLDER AN ACCESS CONSTRAINED ONE ?
NO/YES
55B
OTF?
NO/POINTER
55C
BUBBLE?
NO/POINTER
55D
OTHER?
NO/POINTER(S)
55E
APPLICABLE PERMISSION RULES SET
15
15a
OPEN_AND_GET_FILE_HANDLE (\\SERVER_NAME \ROOT\DIR\SUBDIR \...\FILE_NAME)
READ (HANDLE)
-15b-
WRITE (HANDLE)
-15c-
COPY (HANDLE)
-15d-
CLOSE (HANDLE)
15e
OTF FOLDER
52
BUBBLE FOLDER
54
UNCON-STRAINED FOLDER
53
52b
52a
54b
54a
PERMISSIONS -IDENTIFIER/ PROVIDER
55
57
58
REMOTE FILE REQUEST HANDLER
51
REMOTE OS
59
30'
31
32
30
CHANNEL
34
33
21
11
LOCAL PRO
19
29
LOCAL FILE RQST HANDLER
FILE-ACCESS REQUESTING CLIENT -10-
FILE-ACCESS REQUESTING CLIENT -20-
LOCAL-DISK
12
LOCAL-OS
14
LOCAL-PGM
16
25, 25'
Local Con -strain -ing Mechanisms
LOCAL-DISK
22
LOCAL-OS
24
LOCAL-PGM
26
95

Fig. 1C

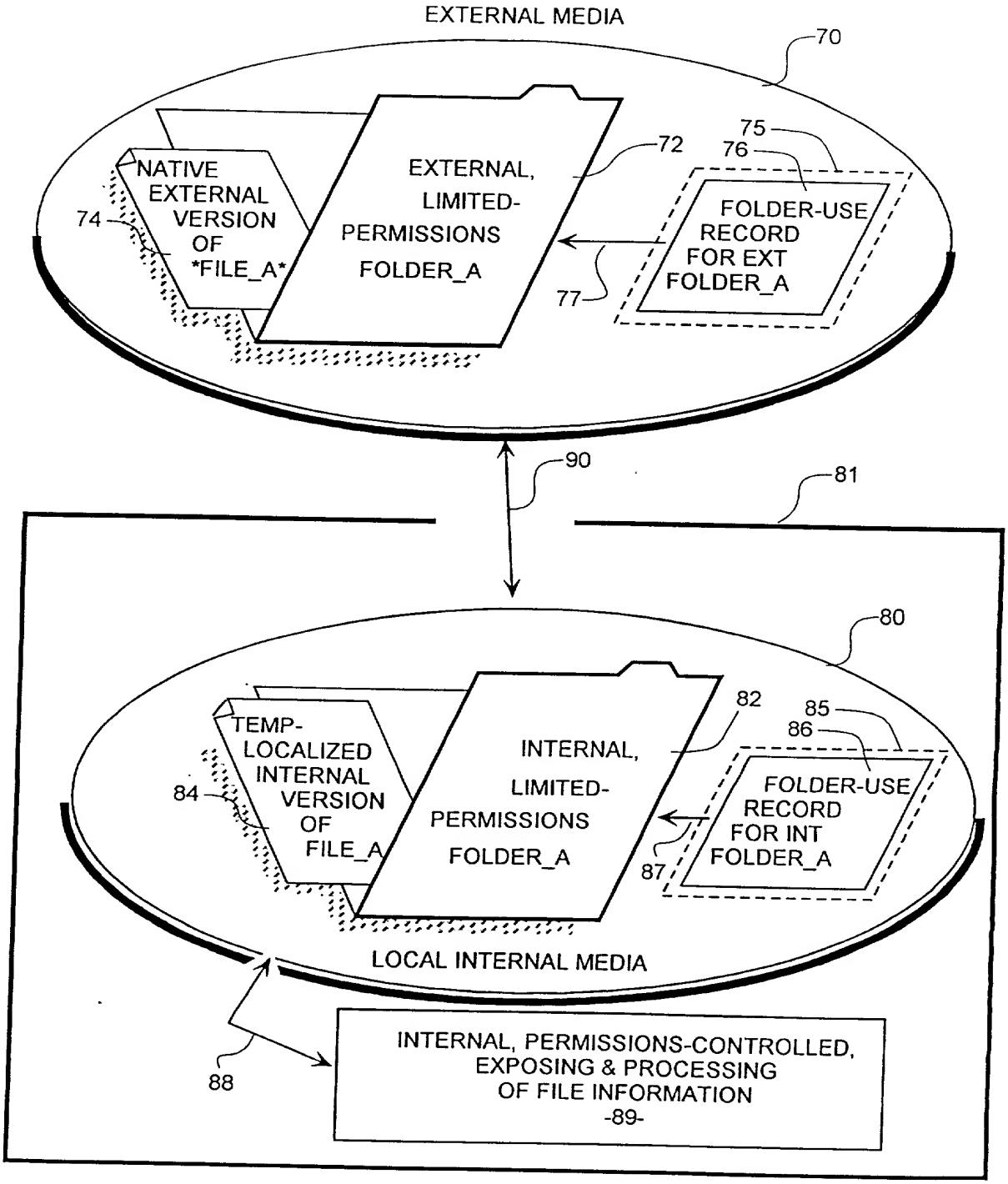

EXTERNAL MEDIA
70
NATIVE EXTERNAL VERSION OF *FILE_A*
74
EXTERNAL, LIMITED-PERMISSIONS FOLDER_A
72
75
76
FOLDER-USE RECORD FOR EXT FOLDER_A
77
90
81
80
TEMP-LOCALIZED INTERNAL VERSION OF FILE_A
84
INTERNAL, LIMITED-PERMISSIONS FOLDER_A
82
85
86
FOLDER-USE RECORD FOR INT FOLDER_A
87
LOCAL INTERNAL MEDIA
88
INTERNAL, PERMISSIONS-CONTROLLED, EXPOSING & PROCESSING OF FILE INFORMATION
-89-

Fig. 1D

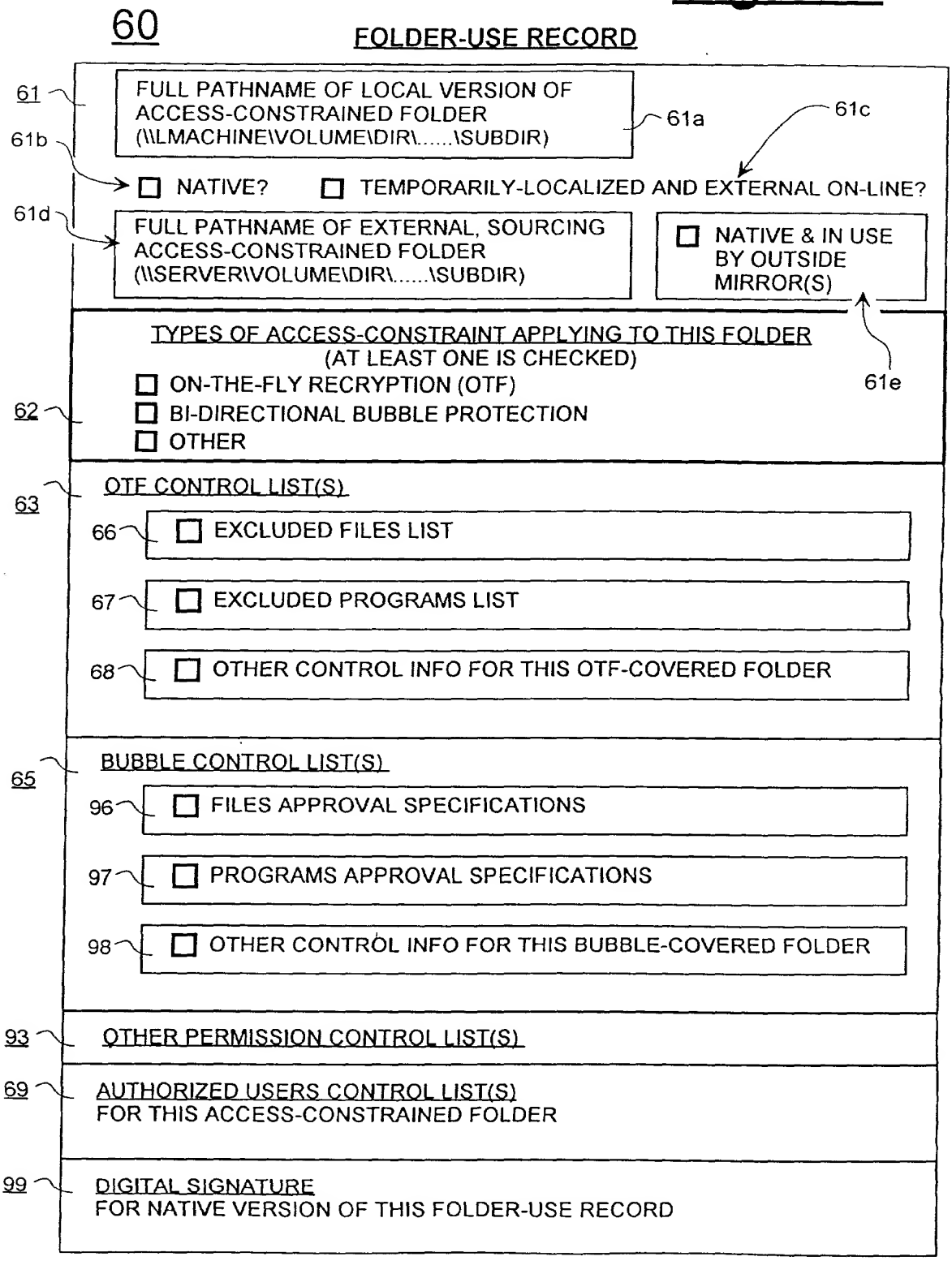
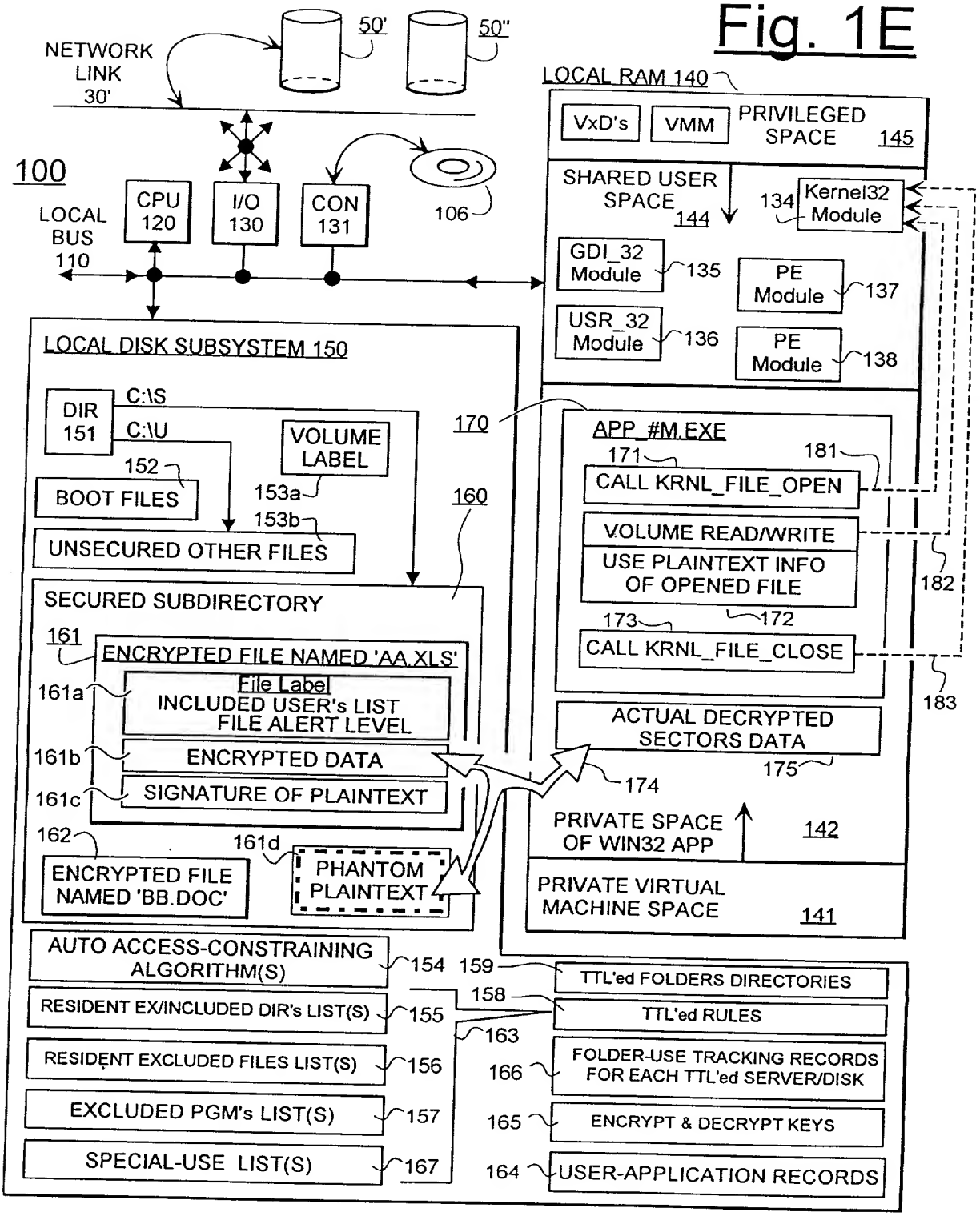

60
FOLDER-USE RECORD
61
FULL PATHNAME OF LOCAL VERSION OF ACCESS-CONSTRAINED FOLDER (\\LMACHINE\VOLUME\DIR\.....\SUBDIR)
61a
61c
61b
NATIVE?
TEMPORARILY-LOCALIZED AND EXTERNAL ON-LINE?
61d
FULL PATHNAME OF EXTERNAL, SOURCING ACCESS-CONSTRAINED FOLDER (\\SERVER\VOLUME\DIR\.....\SUBDIR)
NATIVE & IN USE BY OUTSIDE MIRROR(S)
61e
TYPES OF ACCESS-CONSTRAINT APPLYING TO THIS FOLDER
(AT LEAST ONE IS CHECKED)
62
ON-THE-FLY RECRYPTION (OTF)
BI-DIRECTIONAL BUBBLE PROTECTION
OTHER
63
OTF CONTROL LIST(S)
66
EXCLUDED FILES LIST
67
EXCLUDED PROGRAMS LIST
68
OTHER CONTROL INFO FOR THIS OTF-COVERED FOLDER
65
BUBBLE CONTROL LIST(S)
96
FILES APPROVAL SPECIFICATIONS
97
PROGRAMS APPROVAL SPECIFICATIONS
98
OTHER CONTROL INFO FOR THIS BUBBLE-COVERED FOLDER
93
OTHER PERMISSION CONTROL LIST(S)
69
AUTHORIZED USERS CONTROL LIST(S)
FOR THIS ACCESS-CONSTRAINED FOLDER
99
DIGITAL SIGNATURE
FOR NATIVE VERSION OF THIS FOLDER-USE RECORD

Fig. 1E


NETWORK LINK 30'
50'
50"
100
LOCAL BUS 110
CPU 120
I/O 130
CON 131
106
LOCAL RAM 140
VxD's
VMM
PRIVILEGED SPACE 145
SHARED USER SPACE 144
134
Kernel32 Module
GDI_32 Module
135
PE Module
137
USR_32 Module
136
PE Module
138
LOCAL DISK SUBSYSTEM 150
DIR 151
C:\S
C:\U
VOLUME LABEL
152
BOOT FILES
153a
153b
UNSECURED OTHER FILES
170
160
APP_#M.EXE
171
181
CALL KRNL_FILE_OPEN
VOLUME READ/WRITE
USE PLAINTEXT INFO OF OPENED FILE
182
173
172
CALL KRNL_FILE_CLOSE
183
SECURED SUBDIRECTORY
161
ENCRYPTED FILE NAMED 'AA.XLS'
161a
File Label
INCLUDED USER's LIST
FILE ALERT LEVEL
161b
ENCRYPTED DATA
161c
SIGNATURE OF PLAINTEXT
ACTUAL DECRYPTED SECTORS DATA
175
174
162
ENCRYPTED FILE NAMED 'BB.DOC'
161d
PHANTOM PLAINTEXT
PRIVATE SPACE OF WIN32 APP
142
PRIVATE VIRTUAL MACHINE SPACE
141
AUTO ACCESS-CONSTRAINING ALGORITHM(S)
154
159
TTL'ed FOLDERS DIRECTORIES
158
RESIDENT EX/INCLUDED DIR's LIST(S)
155
TTL'ed RULES
163
RESIDENT EXCLUDED FILES LIST(S)
156
166
FOLDER-USE TRACKING RECORDS FOR EACH TTL'ed SERVER/DISK
EXCLUDED PGM's LIST(S)
157
165
ENCRYPT & DECRYPT KEYS
SPECIAL-USE LIST(S)
167
164
USER-APPLICATION RECORDS

200 Fig. 2A

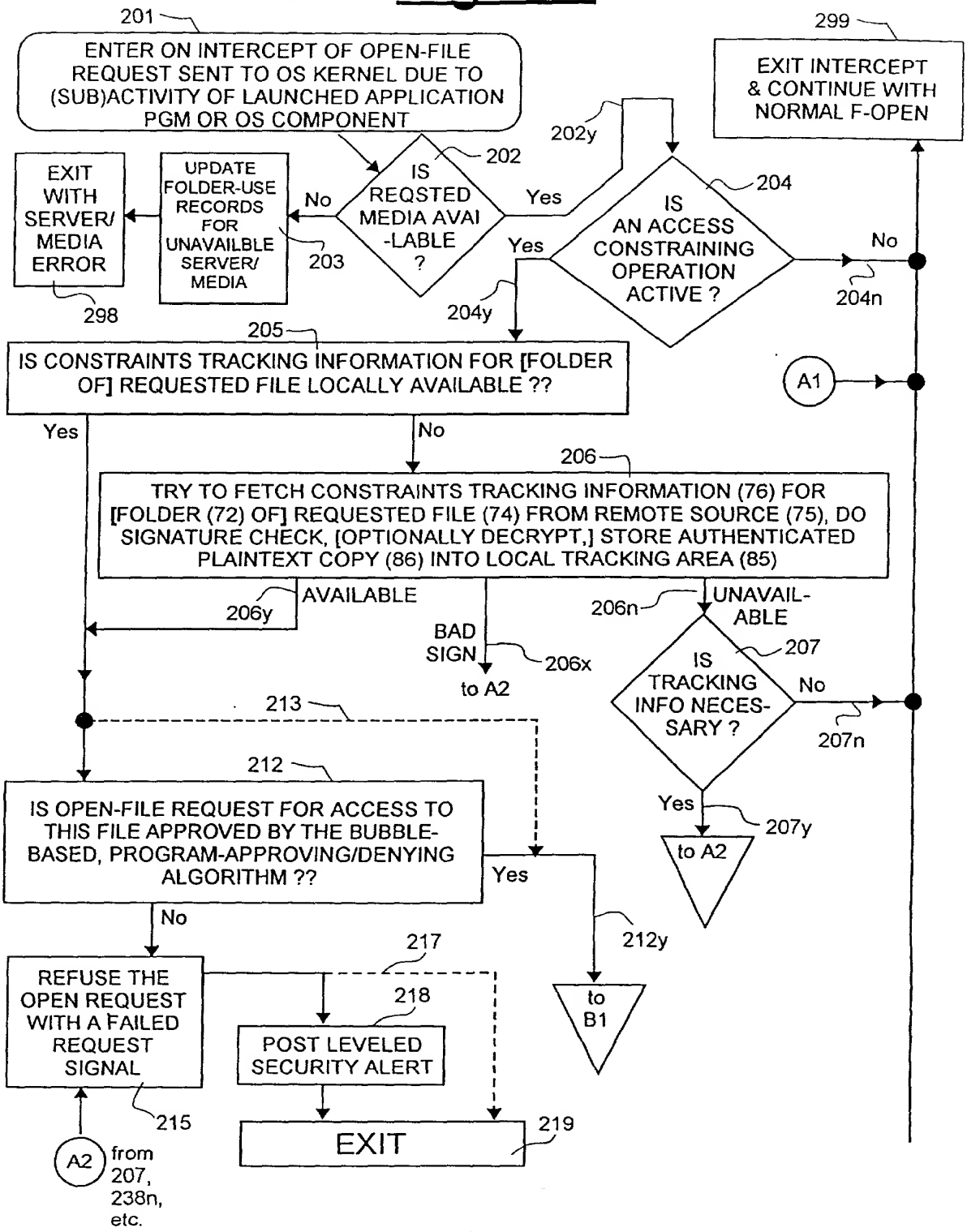

201
ENTER ON INTERCEPT OF OPEN-FILE REQUEST SENT TO OS KERNEL DUE TO (SUB)ACTIVITY OF LAUNCHED APPLICATION PGM OR OS COMPONENT
299
EXIT INTERCEPT & CONTINUE WITH NORMAL F-OPEN
202
IS REQSTED MEDIA AVAI -LABLE ?
202y
Yes
No
UPDATE FOLDER-USE RECORDS FOR UNAVAILBLE SERVER/ MEDIA
203
EXIT WITH SERVER/ MEDIA ERROR
298
204
IS AN ACCESS CONSTRAINING OPERATION ACTIVE ?
Yes
No
204y
204n
205
IS CONSTRAINTS TRACKING INFORMATION FOR [FOLDER OF] REQUESTED FILE LOCALLY AVAILABLE ??
A1
Yes
No
206
TRY TO FETCH CONSTRAINTS TRACKING INFORMATION (76) FOR [FOLDER (72) OF] REQUESTED FILE (74) FROM REMOTE SOURCE (75), DO SIGNATURE CHECK, [OPTIONALLY DECRYPT,] STORE AUTHENTICATED PLAINTEXT COPY (86) INTO LOCAL TRACKING AREA (85)
206y
AVAILABLE
206n
UNAVAIL-ABLE
BAD SIGN
206x
to A2
207
IS TRACKING INFO NECES-SARY ?
No
207n
Yes
207y
to A2
213
212
IS OPEN-FILE REQUEST FOR ACCESS TO THIS FILE APPROVED BY THE BUBBLE-BASED, PROGRAM-APPROVING/DENYING ALGORITHM ??
Yes
212y
No
217
218
REFUSE THE OPEN REQUEST WITH A FAILED REQUEST SIGNAL
POST LEVELED SECURITY ALERT
to B1
215
EXIT
219
A2
from 207, 238n, etc.

Fig. 2B

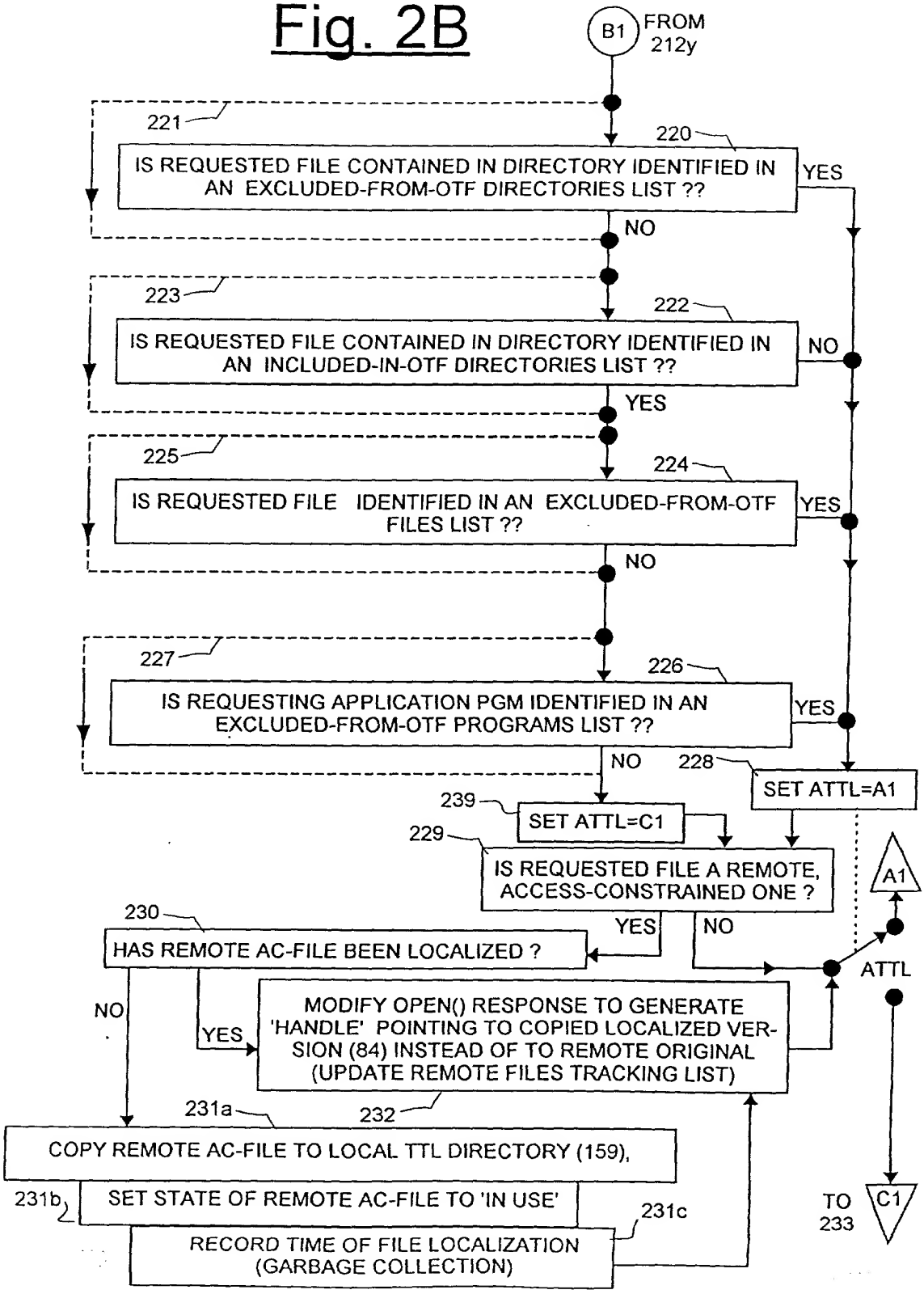
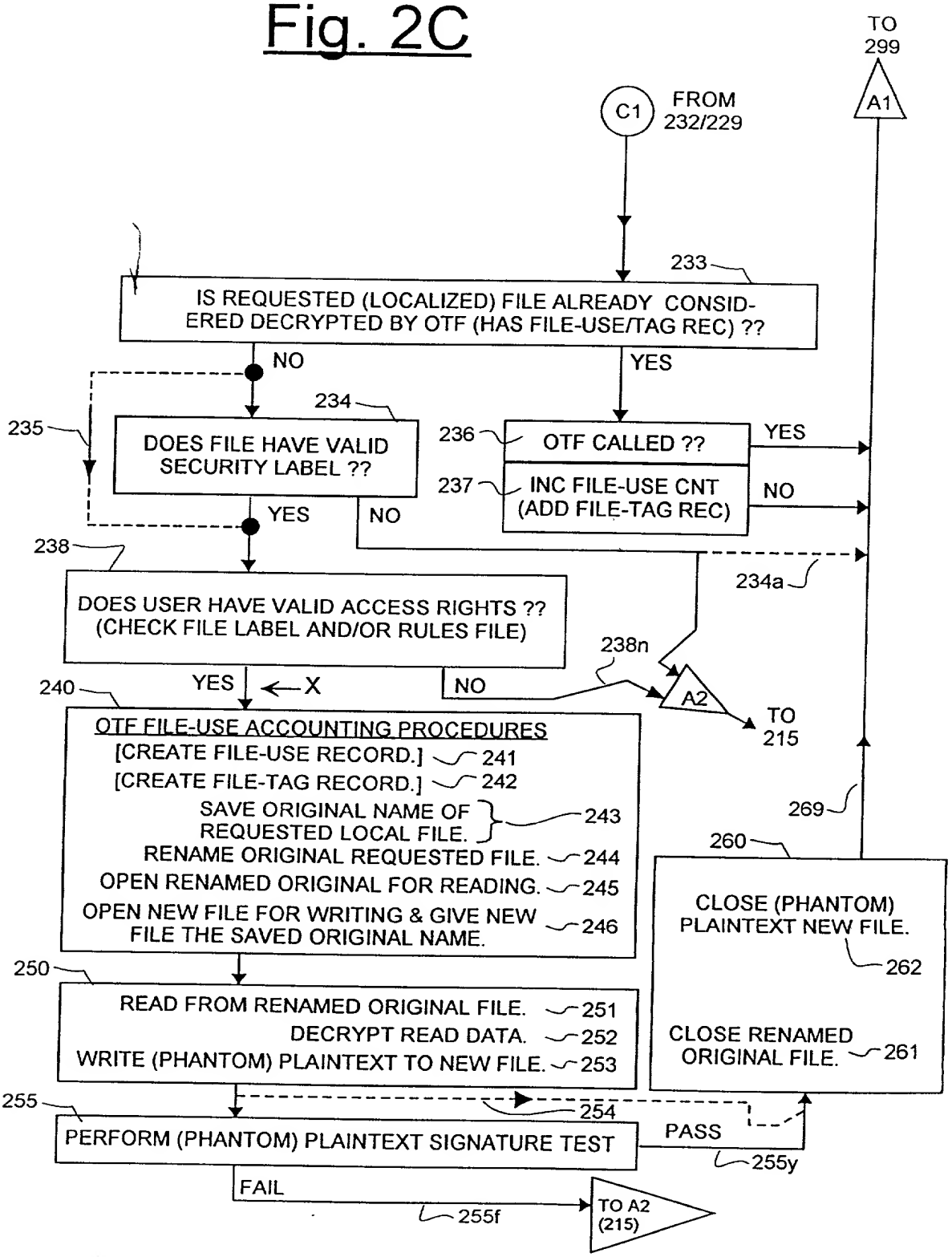

B1
FROM 212y
221
220
IS REQUESTED FILE CONTAINED IN DIRECTORY IDENTIFIED IN AN EXCLUDED-FROM-OTF DIRECTORIES LIST ??
YES
NO
223
222
IS REQUESTED FILE CONTAINED IN DIRECTORY IDENTIFIED IN AN INCLUDED-IN-OTF DIRECTORIES LIST ??
NO
YES
225
224
IS REQUESTED FILE IDENTIFIED IN AN EXCLUDED-FROM-OTF FILES LIST ??
YES
NO
227
226
IS REQUESTING APPLICATION PGM IDENTIFIED IN AN EXCLUDED-FROM-OTF PROGRAMS LIST ??
YES
NO
228
SET ATTL=A1
239
SET ATTL=C1
229
IS REQUESTED FILE A REMOTE, ACCESS-CONSTRAINED ONE ?
A1
230
YES
NO
HAS REMOTE AC-FILE BEEN LOCALIZED ?
ATTL
NO
YES
MODIFY OPEN() RESPONSE TO GENERATE 'HANDLE' POINTING TO COPIED LOCALIZED VERSION (84) INSTEAD OF TO REMOTE ORIGINAL (UPDATE REMOTE FILES TRACKING LIST)
231a
232
COPY REMOTE AC-FILE TO LOCAL TTL DIRECTORY (159),
231b
SET STATE OF REMOTE AC-FILE TO 'IN USE'
231c
RECORD TIME OF FILE LOCALIZATION (GARBAGE COLLECTION)
TO 233
C1

Fig. 2C


TO 299
A1
C1
FROM 232/229
233
IS REQUESTED (LOCALIZED) FILE ALREADY CONSIDERED DECRYPTED BY OTF (HAS FILE-USE/TAG REC) ??
NO
YES
234
235
DOES FILE HAVE VALID SECURITY LABEL ??
236
OTF CALLED ??
YES
237
INC FILE-USE CNT (ADD FILE-TAG REC)
NO
YES
NO
238
234a
DOES USER HAVE VALID ACCESS RIGHTS ?? (CHECK FILE LABEL AND/OR RULES FILE)
238n
240
YES
X
NO
A2
TO 215
OTF FILE-USE ACCOUNTING PROCEDURES
[CREATE FILE-USE RECORD.] 241
[CREATE FILE-TAG RECORD.] 242
SAVE ORIGINAL NAME OF REQUESTED LOCAL FILE. 243
RENAME ORIGINAL REQUESTED FILE. 244
OPEN RENAMED ORIGINAL FOR READING. 245
OPEN NEW FILE FOR WRITING & GIVE NEW FILE THE SAVED ORIGINAL NAME. 246
269
260
CLOSE (PHANTOM) PLAINTEXT NEW FILE. 262
CLOSE RENAMED ORIGINAL FILE. 261
250
READ FROM RENAMED ORIGINAL FILE. 251
DECRYPT READ DATA. 252
WRITE (PHANTOM) PLAINTEXT TO NEW FILE. 253
255
254
PERFORM (PHANTOM) PLAINTEXT SIGNATURE TEST
PASS
255y
FAIL
255f
TO A2 (215)

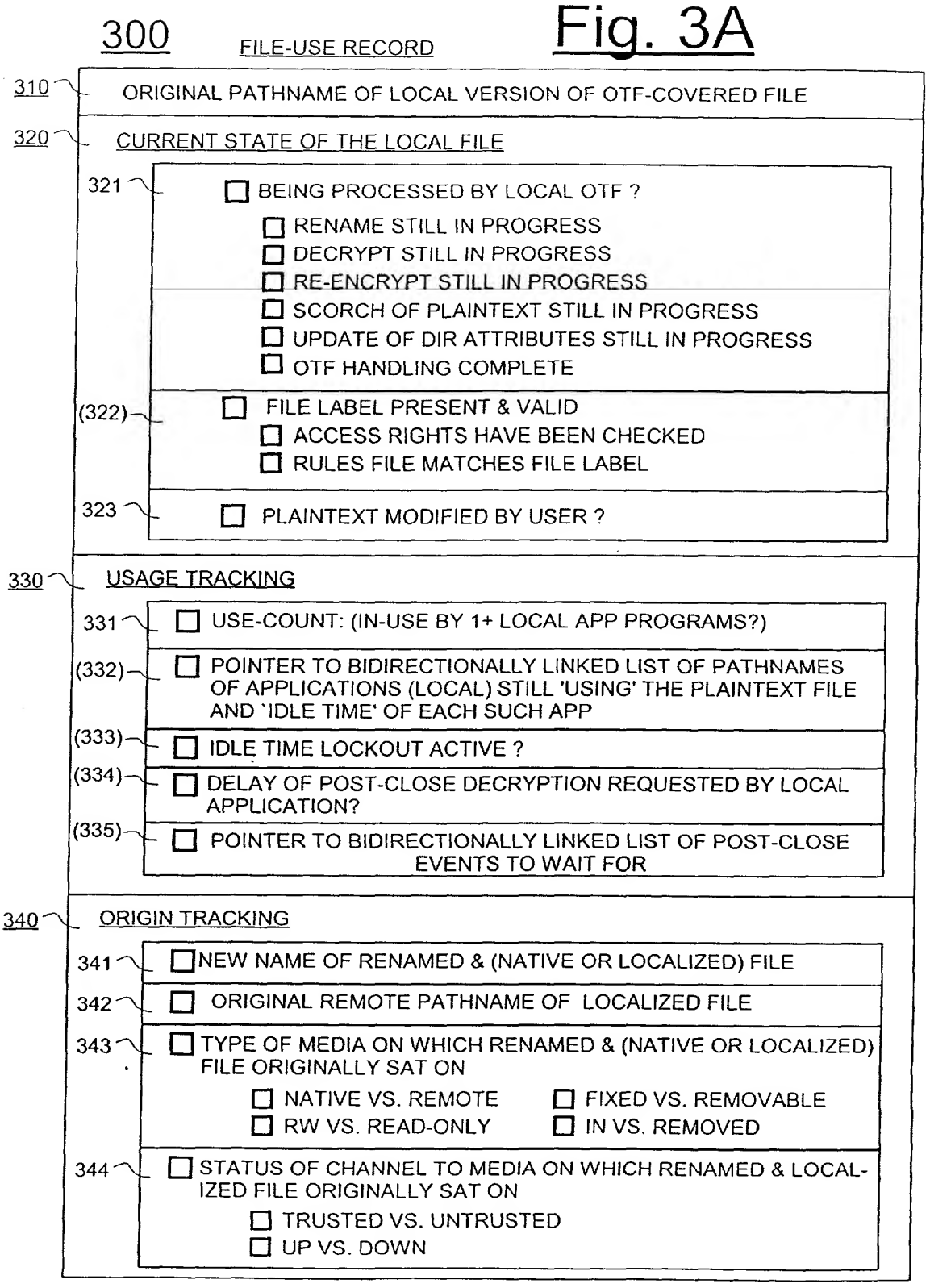

300
FILE-USE RECORD
310
ORIGINAL PATHNAME OF LOCAL VERSION OF OTF-COVERED FILE
320
CURRENT STATE OF THE LOCAL FILE
321
BEING PROCESSED BY LOCAL OTF ?
RENAME STILL IN PROGRESS
DECRYPT STILL IN PROGRESS
RE-ENCRYPT STILL IN PROGRESS
SCORCH OF PLAINTEXT STILL IN PROGRESS
UPDATE OF DIR ATTRIBUTES STILL IN PROGRESS
OTF HANDLING COMPLETE
(322)
FILE LABEL PRESENT & VALID
ACCESS RIGHTS HAVE BEEN CHECKED
RULES FILE MATCHES FILE LABEL
323
PLAINTEXT MODIFIED BY USER ?
330
USAGE TRACKING
331
USE-COUNT: (IN-USE BY 1+ LOCAL APP PROGRAMS?)
(332)
POINTER TO BIDIRECTIONALLY LINKED LIST OF PATHNAMES OF APPLICATIONS (LOCAL) STILL 'USING' THE PLAINTEXT FILE AND `IDLE TIME' OF EACH SUCH APP
(333)
IDLE TIME LOCKOUT ACTIVE ?
(334)
DELAY OF POST-CLOSE DECRYPTION REQUESTED BY LOCAL APPLICATION?
(335)
POINTER TO BIDIRECTIONALLY LINKED LIST OF POST-CLOSE EVENTS TO WAIT FOR
340
ORIGIN TRACKING
341
NEW NAME OF RENAMED & (NATIVE OR LOCALIZED) FILE
342
ORIGINAL REMOTE PATHNAME OF LOCALIZED FILE
343
TYPE OF MEDIA ON WHICH RENAMED & (NATIVE OR LOCALIZED) FILE ORIGINALLY SAT ON
NATIVE VS. REMOTE
FIXED VS. REMOVABLE
RW VS. READ-ONLY
IN VS. REMOVED
344
STATUS OF CHANNEL TO MEDIA ON WHICH RENAMED & LOCALIZED FILE ORIGINALLY SAT ON
TRUSTED VS. UNTRUSTED
UP VS. DOWN

Fig. 3A

Fig. 3B

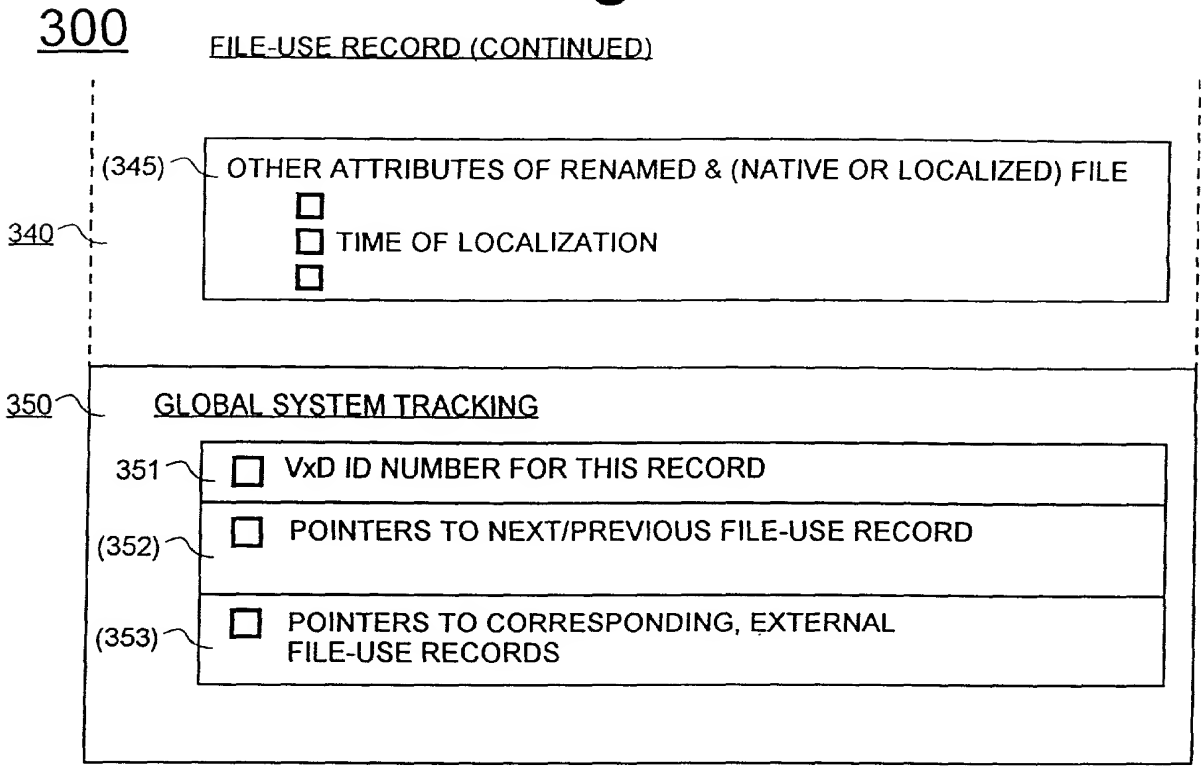

300
FILE-USE RECORD (CONTINUED)
(345)
OTHER ATTRIBUTES OF RENAMED & (NATIVE OR LOCALIZED) FILE
340
TIME OF LOCALIZATION
350
GLOBAL SYSTEM TRACKING
351
VxD ID NUMBER FOR THIS RECORD
(352)
POINTERS TO NEXT/PREVIOUS FILE-USE RECORD
(353)
POINTERS TO CORRESPONDING, EXTERNAL FILE-USE RECORDS

Fig. 3C

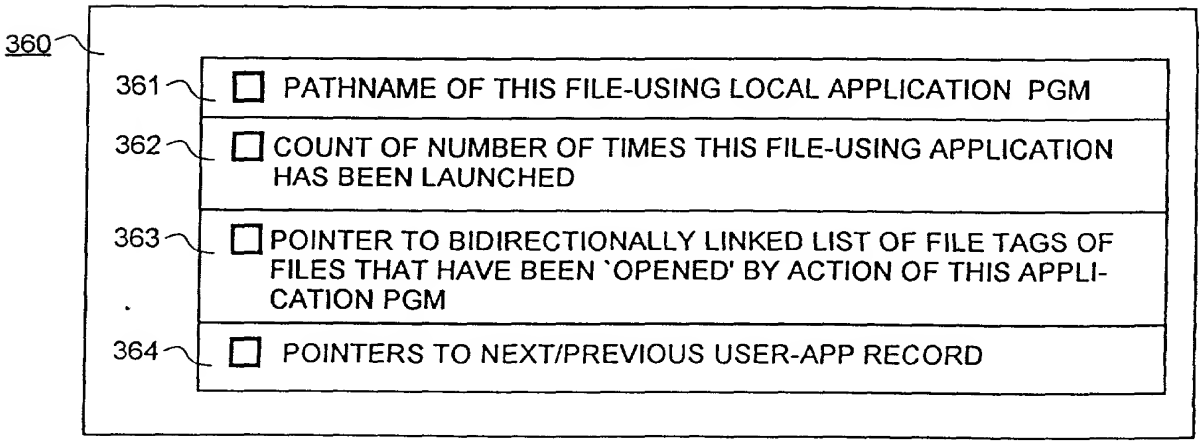
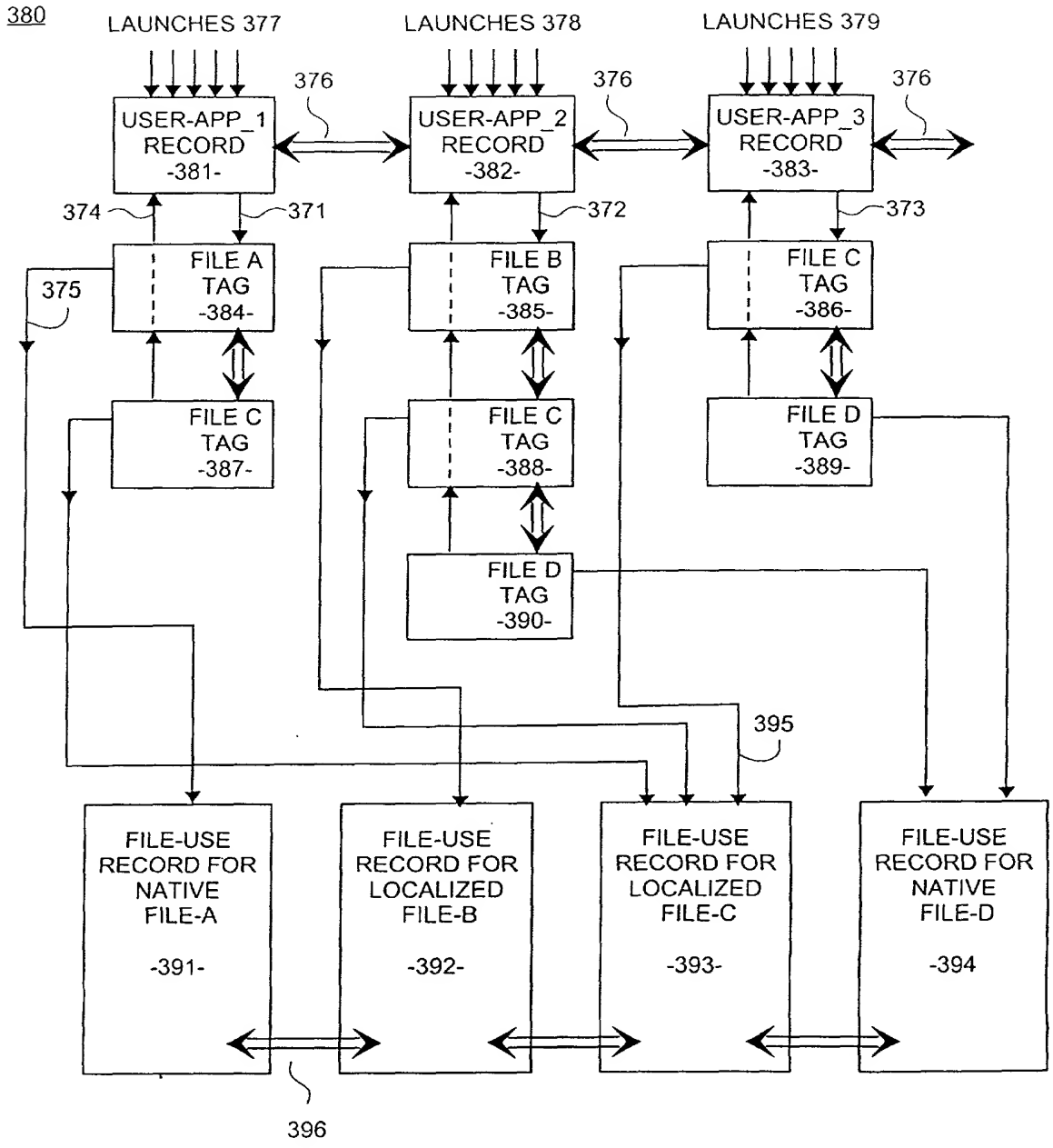

USER-APPLICATION RECORD
360
361
PATHNAME OF THIS FILE-USING LOCAL APPLICATION PGM
362
COUNT OF NUMBER OF TIMES THIS FILE-USING APPLICATION HAS BEEN LAUNCHED
363
POINTER TO BIDIRECTIONALLY LINKED LIST OF FILE TAGS OF FILES THAT HAVE BEEN 'OPENED' BY ACTION OF THIS APPLI-CATION PGM
364
POINTERS TO NEXT/PREVIOUS USER-APP RECORD

Fig. 3D


380
LAUNCHES 377
LAUNCHES 378
LAUNCHES 379
376
376
376
USER-APP_1 RECORD -381-
USER-APP_2 RECORD -382-
USER-APP_3 RECORD -383-
374
371
372
373
375
FILE A TAG -384-
FILE B TAG -385-
FILE C TAG -386-
FILE C TAG -387-
FILE C TAG -388-
FILE D TAG -389-
FILE D TAG -390-
395
FILE-USE RECORD FOR NATIVE FILE-A -391-
FILE-USE RECORD FOR LOCALIZED FILE-B -392-
FILE-USE RECORD FOR LOCALIZED FILE-C -393-
FILE-USE RECORD FOR NATIVE FILE-D -394
396

400 Fig. 4A

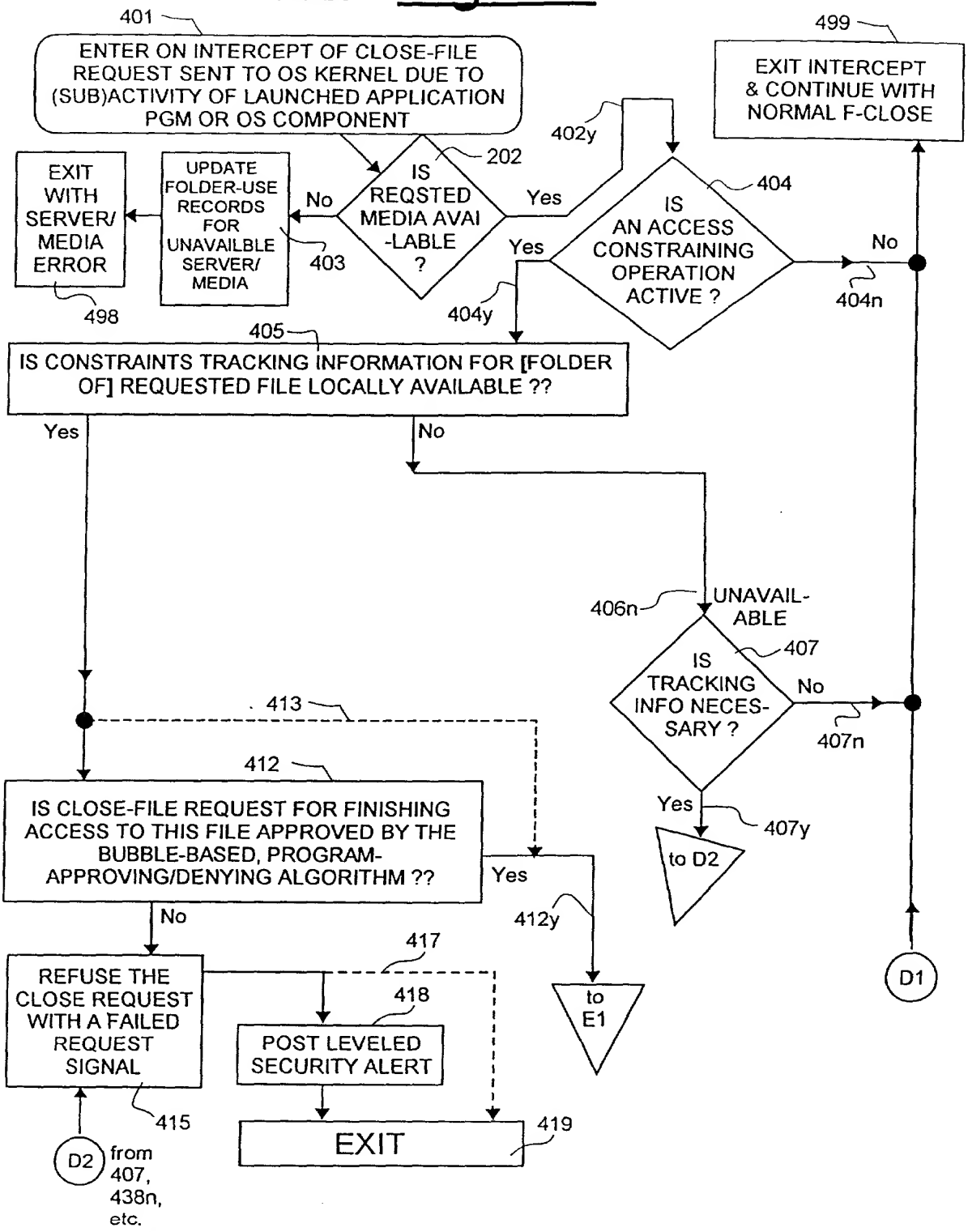

401
ENTER ON INTERCEPT OF CLOSE-FILE REQUEST SENT TO OS KERNEL DUE TO (SUB)ACTIVITY OF LAUNCHED APPLICATION PGM OR OS COMPONENT
499
EXIT INTERCEPT & CONTINUE WITH NORMAL F-CLOSE
202
IS REQSTED MEDIA AVAI -LABLE ?
No
Yes
402y
404
IS AN ACCESS CONSTRAINING OPERATION ACTIVE ?
Yes
No
404y
404n
EXIT WITH SERVER/ MEDIA ERROR
498
UPDATE FOLDER-USE RECORDS FOR UNAVAILBLE SERVER/ MEDIA
403
405
IS CONSTRAINTS TRACKING INFORMATION FOR [FOLDER OF] REQUESTED FILE LOCALLY AVAILABLE ??
Yes
No
406n
UNAVAIL-ABLE
407
IS TRACKING INFO NECES-SARY ?
No
407n
Yes
407y
to D2
413
412
IS CLOSE-FILE REQUEST FOR FINISHING ACCESS TO THIS FILE APPROVED BY THE BUBBLE-BASED, PROGRAM-APPROVING/DENYING ALGORITHM ??
Yes
412y
No
417
418
REFUSE THE CLOSE REQUEST WITH A FAILED REQUEST SIGNAL
POST LEVELED SECURITY ALERT
to E1
D1
415
EXIT
419
D2
from 407, 438n, etc.

Fig. 4B

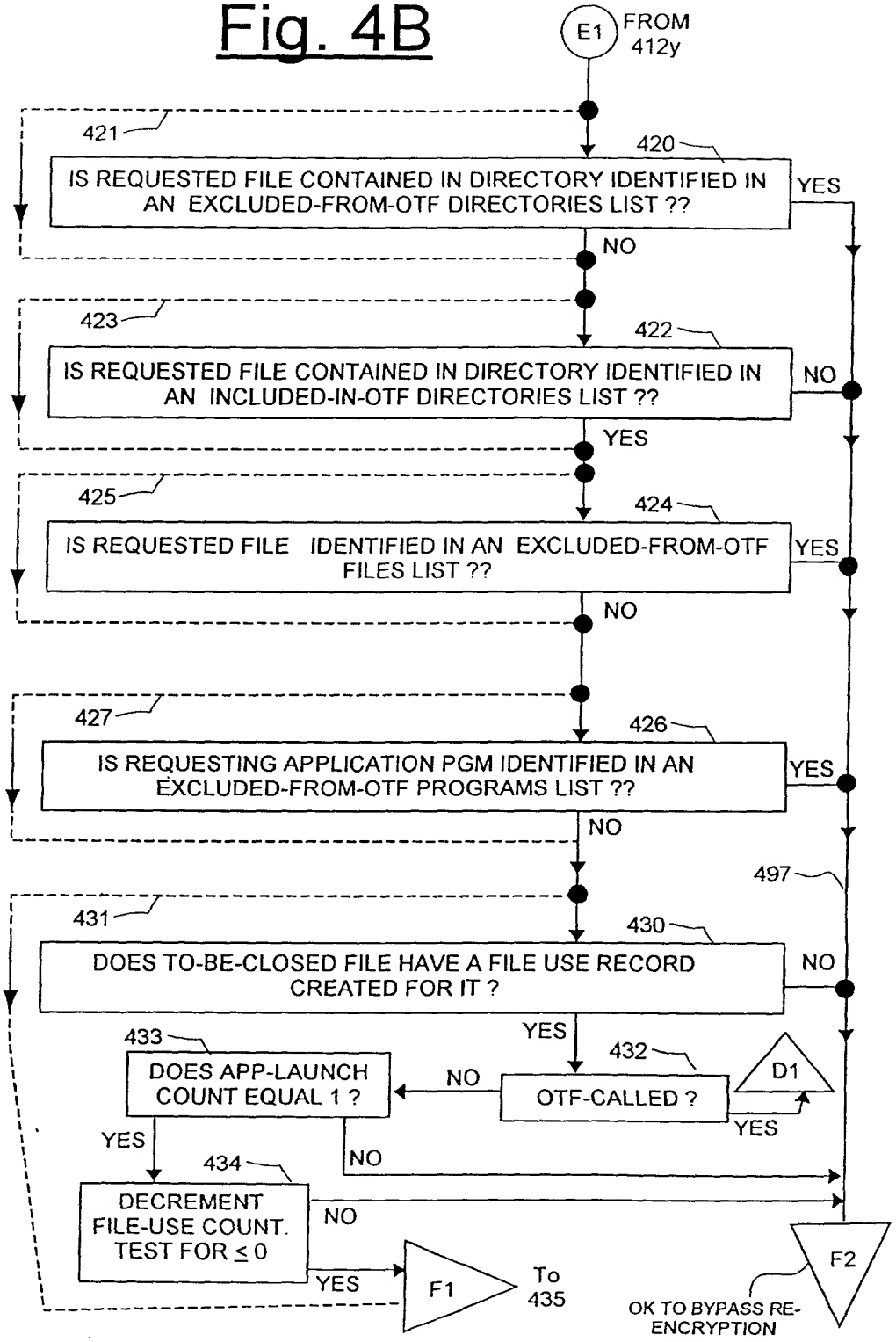

E1
FROM 412y
421
420
IS REQUESTED FILE CONTAINED IN DIRECTORY IDENTIFIED IN AN EXCLUDED-FROM-OTF DIRECTORIES LIST ??
YES
NO
423
422
IS REQUESTED FILE CONTAINED IN DIRECTORY IDENTIFIED IN AN INCLUDED-IN-OTF DIRECTORIES LIST ??
NO
YES
425
424
IS REQUESTED FILE IDENTIFIED IN AN EXCLUDED-FROM-OTF FILES LIST ??
YES
NO
427
426
IS REQUESTING APPLICATION PGM IDENTIFIED IN AN EXCLUDED-FROM-OTF PROGRAMS LIST ??
YES
NO
497
431
430
DOES TO-BE-CLOSED FILE HAVE A FILE USE RECORD CREATED FOR IT ?
NO
YES
433
DOES APP-LAUNCH COUNT EQUAL 1 ?
NO
432
OTF-CALLED ?
D1
YES
YES
NO
434
DECREMENT FILE-USE COUNT. TEST FOR ≤ 0
NO
YES
F1
To 435
F2
OK TO BYPASS RE-ENCRYPTION

Fig. 4C

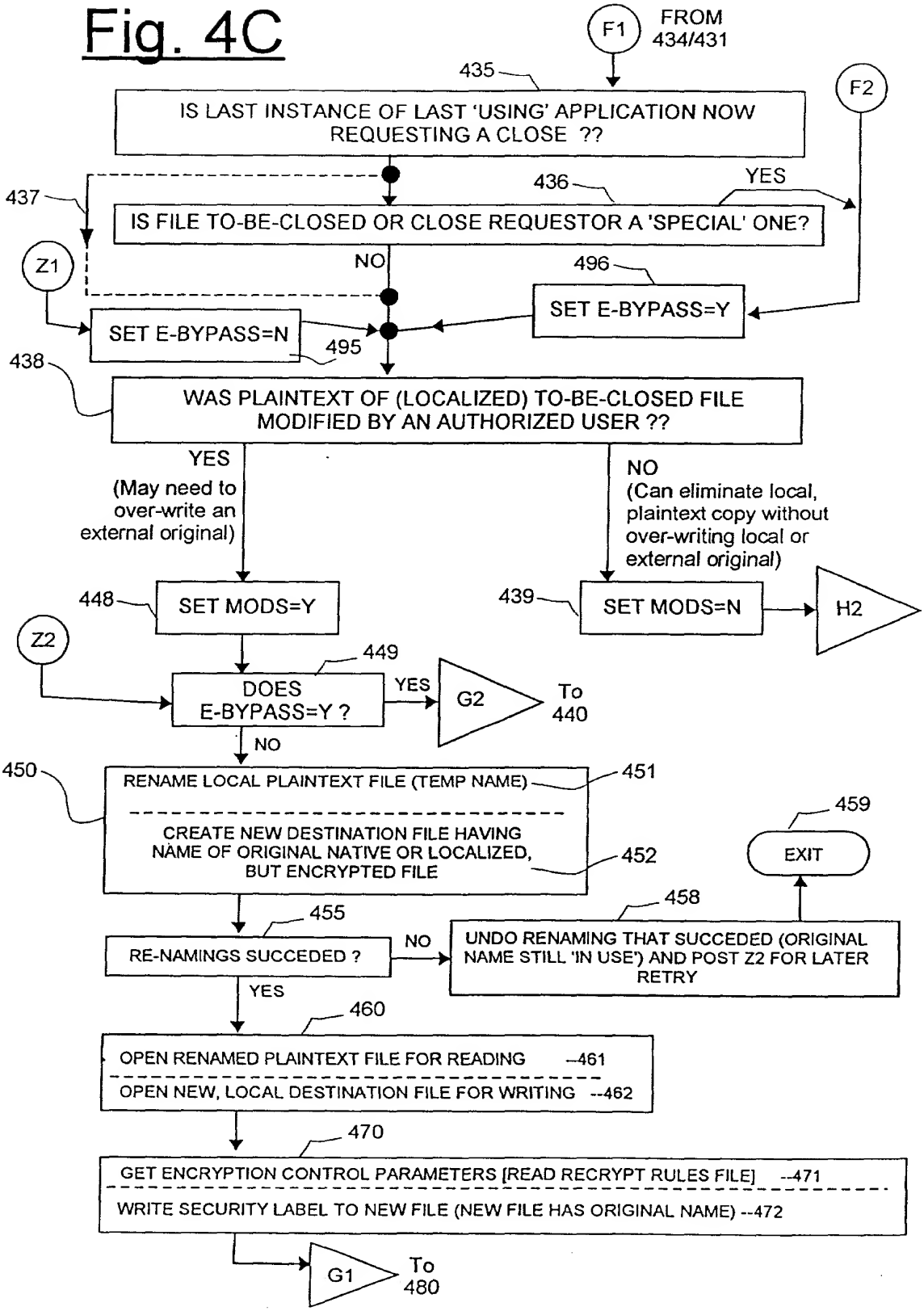

F1
FROM 434/431
435
IS LAST INSTANCE OF LAST 'USING' APPLICATION NOW REQUESTING A CLOSE ??
F2
436
YES
437
IS FILE TO-BE-CLOSED OR CLOSE REQUESTOR A 'SPECIAL' ONE?
NO
496
Z1
SET E-BYPASS=Y
SET E-BYPASS=N
495
438
WAS PLAINTEXT OF (LOCALIZED) TO-BE-CLOSED FILE MODIFIED BY AN AUTHORIZED USER ??
YES
(May need to over-write an external original)
NO
(Can eliminate local, plaintext copy without over-writing local or external original)
448
SET MODS=Y
439
SET MODS=N
H2
Z2
449
DOES E-BYPASS=Y ?
YES
G2
To 440
NO
450
RENAME LOCAL PLAINTEXT FILE (TEMP NAME)
451
CREATE NEW DESTINATION FILE HAVING NAME OF ORIGINAL NATIVE OR LOCALIZED, BUT ENCRYPTED FILE
452
459
EXIT
458
455
RE-NAMINGS SUCCEDED ?
NO
UNDO RENAMING THAT SUCCEDED (ORIGINAL NAME STILL 'IN USE') AND POST Z2 FOR LATER RETRY
YES
460
OPEN RENAMED PLAINTEXT FILE FOR READING --461
OPEN NEW, LOCAL DESTINATION FILE FOR WRITING --462
470
GET ENCRYPTION CONTROL PARAMETERS [READ RECRYPT RULES FILE] --471
WRITE SECURITY LABEL TO NEW FILE (NEW FILE HAS ORIGINAL NAME) --472
G1
To 480

Fig. 4D

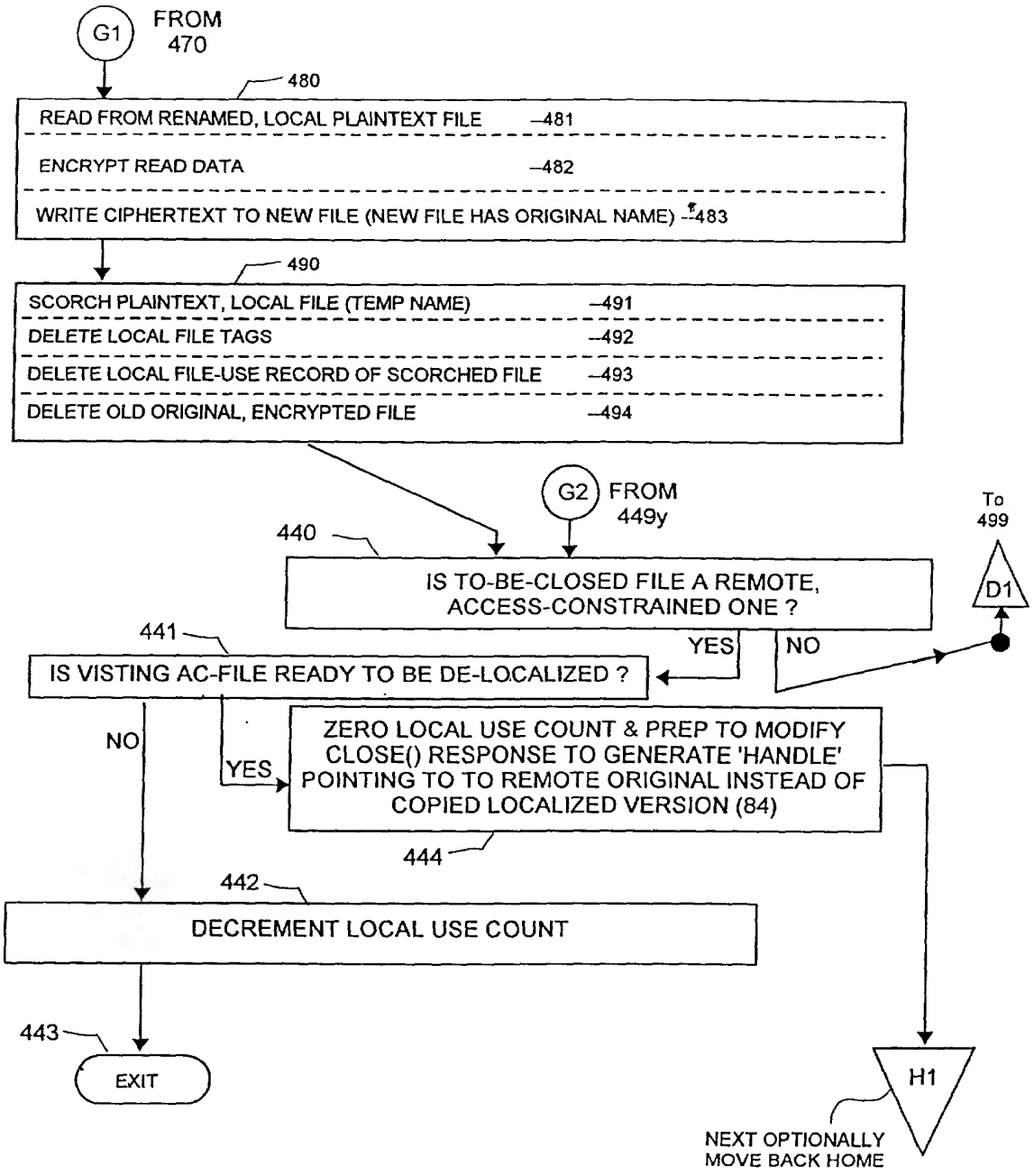
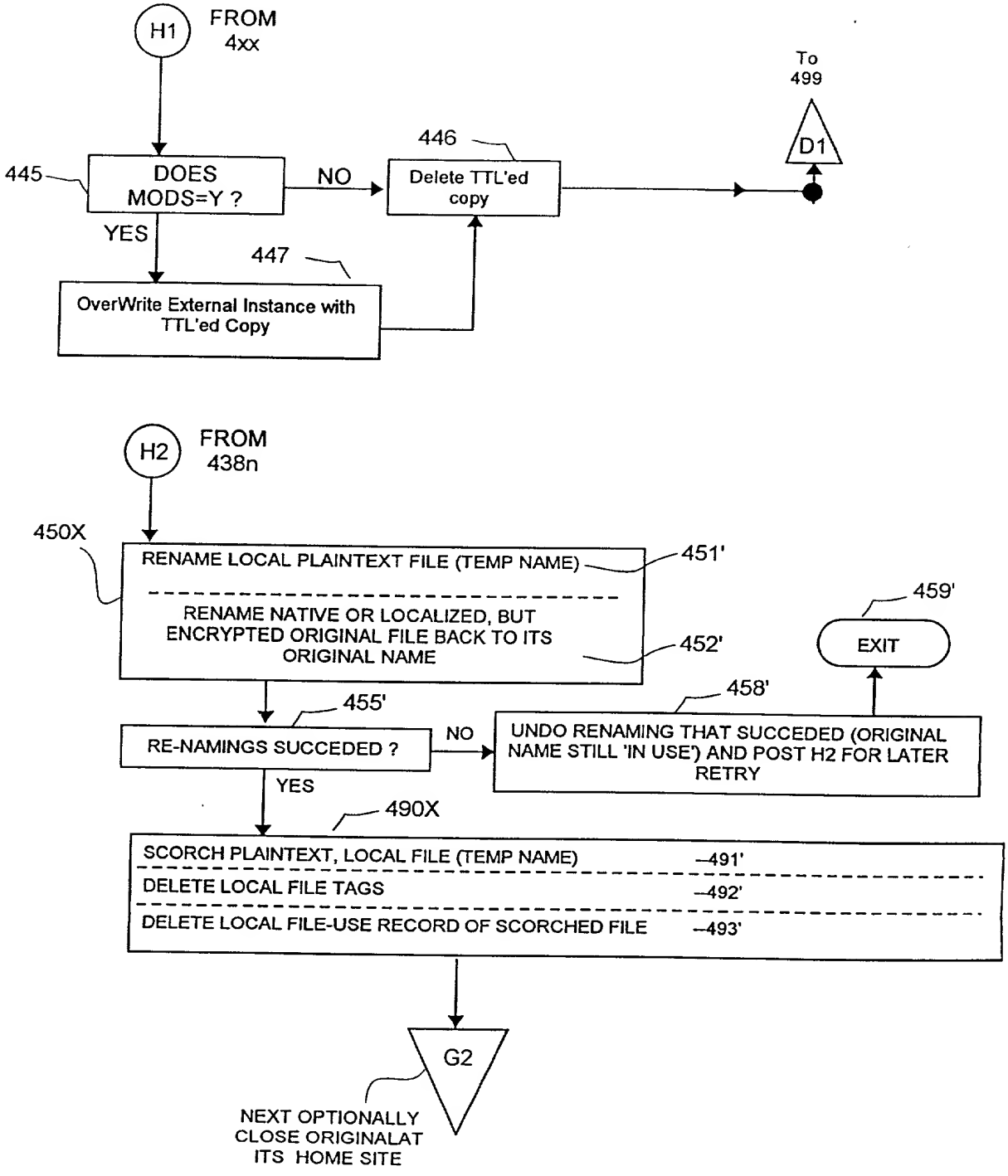

G1
FROM 470
480
READ FROM RENAMED, LOCAL PLAINTEXT FILE —481
ENCRYPT READ DATA —482
WRITE CIPHERTEXT TO NEW FILE (NEW FILE HAS ORIGINAL NAME) —483
490
SCORCH PLAINTEXT, LOCAL FILE (TEMP NAME) —491
DELETE LOCAL FILE TAGS —492
DELETE LOCAL FILE-USE RECORD OF SCORCHED FILE —493
DELETE OLD ORIGINAL, ENCRYPTED FILE —494
G2
FROM 449y
To 499
D1
440
IS TO-BE-CLOSED FILE A REMOTE, ACCESS-CONSTRAINED ONE ?
YES
NO
441
IS VISTING AC-FILE READY TO BE DE-LOCALIZED ?
NO
YES
ZERO LOCAL USE COUNT & PREP TO MODIFY CLOSE() RESPONSE TO GENERATE 'HANDLE' POINTING TO TO REMOTE ORIGINAL INSTEAD OF COPIED LOCALIZED VERSION (84)
444
442
DECREMENT LOCAL USE COUNT
443
EXIT
H1
NEXT OPTIONALLY MOVE BACK HOME

Fig. 4E


H1
FROM 4xx
To 499
D1
446
445
DOES MODS=Y ?
NO
Delete TTL'ed copy
YES
447
OverWrite External Instance with TTL'ed Copy
H2
FROM 438n
450X
RENAME LOCAL PLAINTEXT FILE (TEMP NAME)
451'
RENAME NATIVE OR LOCALIZED, BUT ENCRYPTED ORIGINAL FILE BACK TO ITS ORIGINAL NAME
452'
459'
EXIT
455'
458'
RE-NAMINGS SUCCEDED ?
NO
UNDO RENAMING THAT SUCCEDED (ORIGINAL NAME STILL 'IN USE') AND POST H2 FOR LATER RETRY
YES
490X
SCORCH PLAINTEXT, LOCAL FILE (TEMP NAME)
491'
DELETE LOCAL FILE TAGS
492'
DELETE LOCAL FILE-USE RECORD OF SCORCHED FILE
493'
G2
NEXT OPTIONALLY CLOSE ORIGINALAT ITS HOME SITE

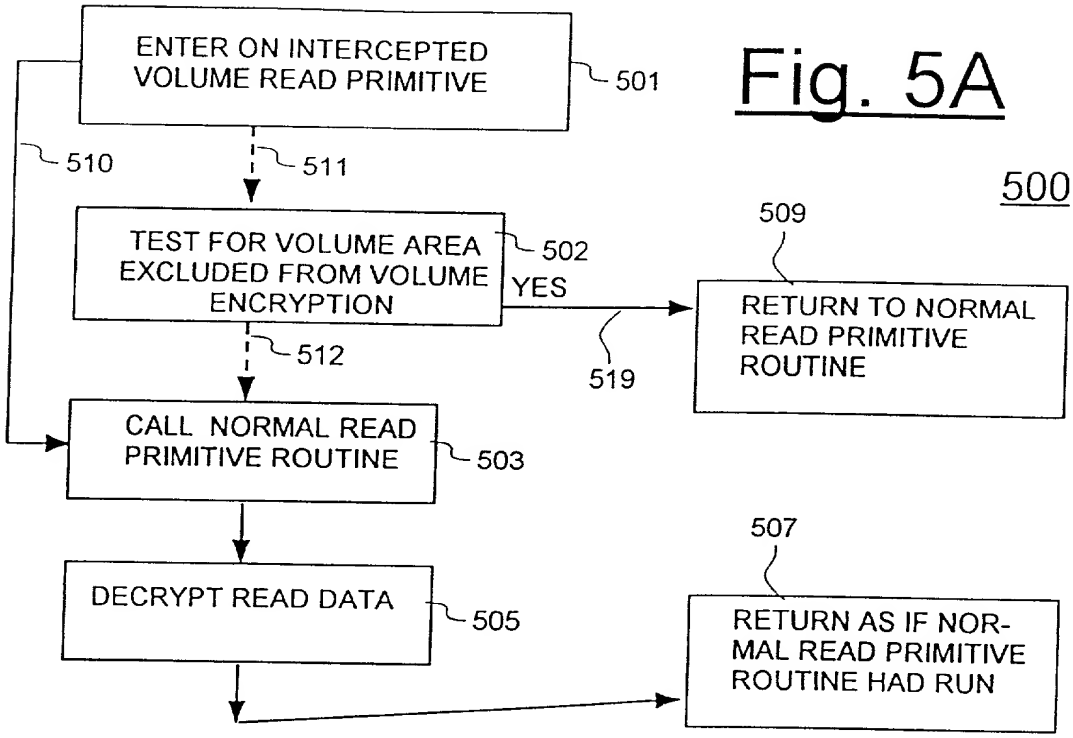

ENTER ON INTERCEPTED VOLUME READ PRIMITIVE
501
510
511
500
TEST FOR VOLUME AREA EXCLUDED FROM VOLUME ENCRYPTION
502
YES
509
RETURN TO NORMAL READ PRIMITIVE ROUTINE
512
519
CALL NORMAL READ PRIMITIVE ROUTINE
503
DECRYPT READ DATA
505
507
RETURN AS IF NORMAL READ PRIMITIVE ROUTINE HAD RUN

Fig. 5A

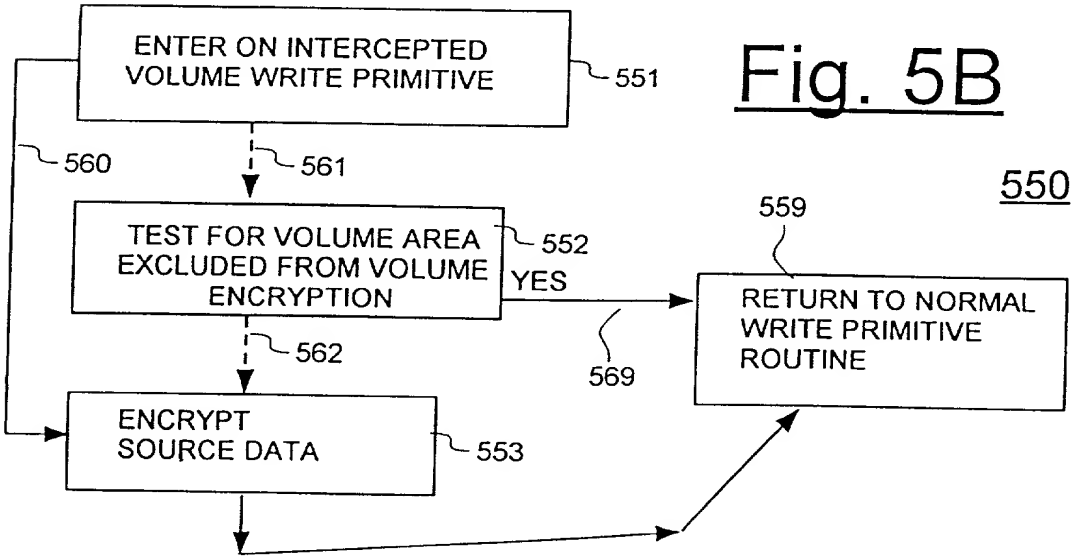
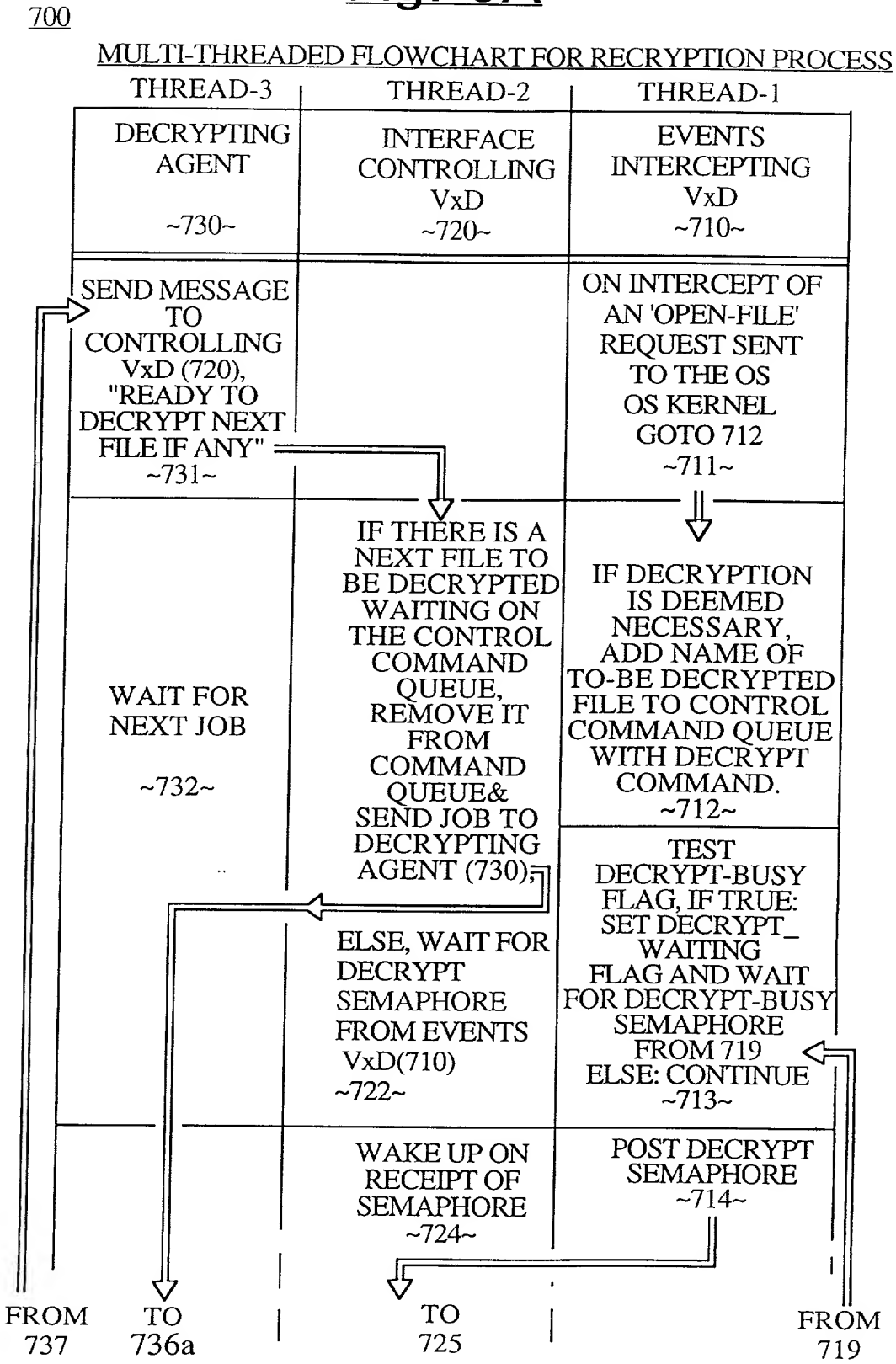

ENTER ON INTERCEPTED VOLUME WRITE PRIMITIVE
551
560
561
550
TEST FOR VOLUME AREA EXCLUDED FROM VOLUME ENCRYPTION
552
YES
559
RETURN TO NORMAL WRITE PRIMITIVE ROUTINE
562
569
ENCRYPT SOURCE DATA
553

Fig. 5B

Fig. 6A


700
MULTI-THREADED FLOWCHART FOR RECRYPTION PROCESS
THREAD-3
THREAD-2
THREAD-1
DECRYPTING AGENT ~730~
INTERFACE CONTROLLING VxD ~720~
EVENTS INTERCEPTING VxD ~710~
SEND MESSAGE TO CONTROLLING VxD (720), "READY TO DECRYPT NEXT FILE IF ANY" ~731~
ON INTERCEPT OF AN 'OPEN-FILE' REQUEST SENT TO THE OS OS KERNEL GOTO 712 ~711~
WAIT FOR NEXT JOB ~732~
IF THERE IS A NEXT FILE TO BE DECRYPTED WAITING ON THE CONTROL COMMAND QUEUE, REMOVE IT FROM COMMAND QUEUE& SEND JOB TO DECRYPTING AGENT (730);
IF DECRYPTION IS DEEMED NECESSARY, ADD NAME OF TO-BE DECRYPTED FILE TO CONTROL COMMAND QUEUE WITH DECRYPT COMMAND. ~712~
TEST DECRYPT-BUSY FLAG, IF TRUE: SET DECRYPT_ WAITING FLAG AND WAIT FOR DECRYPT-BUSY SEMAPHORE FROM 719 ELSE: CONTINUE ~713~
ELSE, WAIT FOR DECRYPT SEMAPHORE FROM EVENTS VxD(710) ~722~
WAKE UP ON RECEIPT OF SEMAPHORE ~724~
POST DECRYPT SEMAPHORE ~714~
FROM 737
TO 736a
TO 725
FROM 719

Applicant: David Grawrock et al.
Serial No.: 09/934,926, filed 08/21/01
Atty Docket No.: SYMA-01045US0MCF/GGG

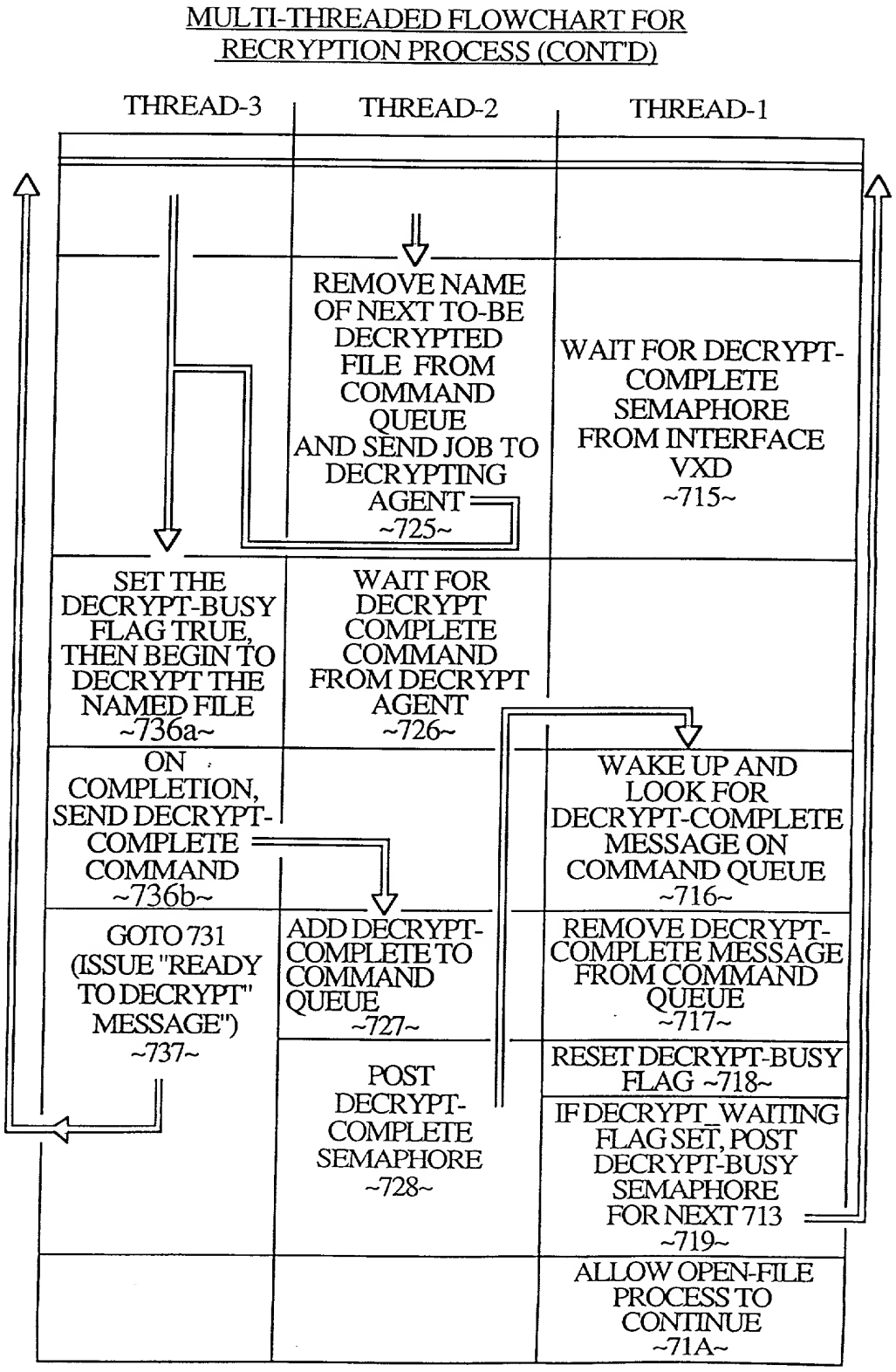



Fig. 6B